What is claimed is:

1. A method comprising:

initiating an operation in a second portion of a system if a value indicates that a first portion of the system is in a trusted state.

2. The method of claim 1, wherein the operation comprises an information update.

3. The method of claim 2, further comprising setting a register containing the value using the first portion before exiting the trusted state.

4. The method of claim 3, further comprising reading the value using the second portion.

5. The method of claim 1, further comprising not performing the operation if the value is not indicative of the trusted state.

6. The method of claim 1, further comprising initiating remediation if the value is not indicative of the trusted state.

7. The method of claim 2, further comprising receiving the information update via an air interface with

the second portion and providing the information update to the first portion.

8. The method of claim 1, wherein the second portion comprises a communications processor of a wireless device and the first portion comprises an applications processor of the wireless device.

9. A method comprising:

maintaining a hardware asset to indicate a trust state of a first subsystem of a system.

10. The method of claim 9, further comprising accessing the hardware asset using a second subsystem of the system.

11. The method of claim 9, wherein the system comprises a wireless device.

12. The method of claim 10, further comprising updating digital content in the second subsystem if the hardware asset indicates the trust state is valid.

13. The method of claim 10, further comprising preventing updating the second subsystem if the hardware asset does not indicate the trust state is valid.

14. The method of claim 13, further comprising performing a remediation measure using the second subsystem if the trust state is not valid.

15. The method of claim 13, further comprising providing an indication to the first subsystem if an update was attempted when the trust state was not valid.

16. The method of claim 9, further comprising setting the hardware asset via the first subsystem before exiting a trusted state, wherein the hardware asset comprises a one-way register.

17. The method of claim 10, further comprising determining if an update is trusted in the first subsystem and transferring the update to the second subsystem if the hardware asset indicates the trust state is valid.

18. An apparatus comprising:

a hardware asset to indicate a trust state of an applications portion of the apparatus.

19. The apparatus of claim 18, wherein the hardware asset is accessible by a communications portion of a wireless device.

20. The apparatus of claim 19, wherein the communications portion cannot modify a value of the hardware asset.

21. The apparatus of claim 18, wherein the hardware asset is coupled to receive a program signal if the trust state of the applications portion is not valid.

22. The apparatus of claim 18, wherein the hardware asset is coupled to receive a reset signal to initiate a trusted state.

23. The apparatus of claim 18, wherein the hardware asset comprises a one-way register.

24. A system comprising:

a hardware asset to indicate a trust state of an applications portion of the system; and

a wireless interface coupled to the hardware asset.

25. The system of claim 24, wherein the hardware asset is accessible by a communications portion of the system, wherein the system comprises a wireless device.

26. The system of claim 24, wherein the hardware asset comprises a one-way register.

27. The system of claim 24, wherein the wireless interface comprises an antenna.

28. An article including a machine-accessible storage medium containing instructions that if executed enable a system to:

control a hardware asset of the system to indicate a trust state of a first portion of the system.

29. The article of claim 28, further comprising instructions that if executed enable the system to update a second portion of the system if the hardware asset indicates the trust state is valid.

30. The article of claim 28, further comprising instructions that if executed enable the system to prevent or discard an update to a second portion of the system if the hardware asset indicates the trust state is not valid.

31. The article of claim 30, further comprising instructions that if executed enable the second portion to initiate a remediation operation if the hardware asset indicates the trust state is not valid.

32. The article of claim 28, further comprising instructions that if executed enable the system to perform a secure operation in a second portion of the system if the hardware asset indicates the trust state is valid.

33. The article of claim 28, further comprising instructions that if executed enable the first portion to vector into a trusted state before initiating a transfer operation to a second portion of the system.

34. A method comprising:

accessing a value with a second portion of a system, the value indicative of a trust state of a first portion of the system.

35. The method of claim 34, further comprising initiating an operation in the second portion if the value is indicative of the trust state.

36. The method of claim 35, wherein the operation comprises an information update.

37. The method of claim 34, wherein the first portion comprises an applications portion of a wireless device and

the second portion comprises a communications portion of the wireless device.